iconectiv

Louise L M Tucker
VP Regulatory and Senior Counsel
m 202.368.5180
ltucker@iconectiv.com | iconectiv.com

October 13, 2016

Ex Parte

Marlene H. Dortch
Secretary
Federal Communications Commission
445 Twelfth Street, S.W.
Washington, DC 20554

Re: *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106

Dear Ms. Dortch:

Telcordia Technologies, Inc.,[1] doing business as iconectiv ("Telcordia" or "iconectiv"), has been a major architect of the United States' telecommunications system since it was formed at the divestiture of AT&T in 1983. We have first-hand knowledge of the intricacies and complexities of creating, operating, and securing the country's telecommunications infrastructure. On July 25, 2016 the FCC released its Order[2] approving the North American Numbering Council (NANC) recommendation that iconectiv serve as the next Local Number Portability Administrator (LNPA) for the United States.

[1] Since February 14, 2013, Telcordia, a wholly owned subsidiary of Ericsson, has been doing business as iconectiv. Telcordia is a US-based company.

[2] *See In the Matters of Telcordia Technologies, Inc Petition to Reform Amendment 57 and to Order a Competitive Bidding Process for Number Portability Administration and Petition of Telcordia Technologies, Inc to Reform or Strike Amendment 70, to Institute Competitive Bidding for Number Portability Administration,* and *to End the NAPM LLC's Interim Role in Number Portability Administration Contract Management,* Order, WC Docket No. 07-149, WC Docket No. 09-109, CC Docket No. 95-116, FCC 16-92, released July 25, 2016.

In our recent discussions with FCC staff regarding the Commission's ongoing privacy proceeding, we noted that the Commission's proposals in the Notice of Proposed Rulemaking regarding *permissionless* use and sharing of customer proprietary network information ("CPNI") and customer proprietary information ("CPI") were, in some instances, ambiguous.[3] Neither the FCC Fact Sheet nor the FCC blog[4] by FCC Chairman Wheeler, both released October 6, 2016, appear to resolve these ambiguities. Thus, we believe it is important to reiterate our position that while we support the *permissionless* sharing of CPNI and CPI for the purposes described in the FCC's proposal, we believe that Congressional intent, consumer expectations, and consumer protection require the FCC to remove all ambiguities that could prevent carriers from using or disclosing *any* data protected by Section 222 in order to prevent customer account takeover ("ATO") and other fraudulent practices. Specifically, the Commission should update its rules to:

(1) interpret Section 222(d), which enumerates a number of exemptions from the requirement that carriers only use CPNI as "required by law or with the approval of the customer,"[5] to apply to all categories of data protected by Section 222, not just CPNI;

(2) clarify that all telecommunications and interconnected VoIP providers, in addition to BIAS providers, can use data covered by Section 222 to prevent and respond to fraud and other unlawful activities; and

(3) make explicit that permissionless disclosure covered by the Commission's rules implementing Section 222(d) can be made available to all of the third parties that assist in preventing and responding to ATO and other forms of fraud or unlawful activity.

Customers are adopting a growing range of mobile and digital experiences that leverage their mobile identities. As we explained in our comments in this proceeding, authentication mechanisms commonly use mobile identity, but it is vulnerable to a variety of security

---

3 *See Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, Notice of Proposed Rulemaking, 31 FCC Rcd. 2500, 2541-42 ¶¶ 117-119 (2016) ("*BIAS CPNI NPRM*").

4 *"Protecting Privacy for Broadband Consumers", https://www.fcc.gov/news-events/blog/2016/10/06/protecting-privacy-broadband-consumers, FACT SHEET: CHAIRMAN WHEELER'S PROPOSAL TO GIVE BROADBAND CONSUMERS INCREASED CHOICE OVER THEIR PERSONAL INFORMATION, WCB DOC-341633A1.docx; Oct. 6, 2016*

5 47 U.S.C. § 222(c).

threats.[6] Fraudsters have been able to use porting, SIM swapping, forwarding, and other social engineering exploits to effect a customer account status change that can compromise customers' mobile identities, access confidential data, take over their financial accounts, and effectuate fraudulent transactions.[7]

BIAS providers and traditional (legacy) communication service providers ("CSPs") can work with their trusted third-party fraud prevention providers to prevent fraud and abuse, including ATO. But in order to protect many different types of customers' confidential data, such as health care or financial data, carriers must be able to use and disclose information protected by Section 222. This information must be disclosed *quickly* to entities with whom the customer does business—such as hospitals, health insurance providers, and financial institutions—to be able to keep up with identity thieves. Because speed is of the essence in preventing ATO, BIAS providers and traditional CSPs need to be expressly permitted to disclose information covered by Section 222 *without prior permission* for the purposes of protecting consumers from fraud. Absent such sharing in a timely manner, carriers will not be able to protect customers from fraud and other abuses as effectively as possible. Thus, it is essential that carriers be able to engage in *permissionless* sharing of information when doing so is reasonably necessary to prevent or respond to ATO and other forms of fraud.

As discussed in our comments in this proceeding, carriers need to be able to quickly share not only CPNI, but also other forms of personally identifiable information, which may be protected by Section 222 even if it does not qualify as CPNI. Much of this data falls under the

---

[6] Comments of Telcordia Technologies, Inc. d/b/a iconectiv at 3, WC Docket No. 16-106 (filed May 27, 2016).

[7] *See, e.g.*, Lorrie Cranor, *Your Mobile Phone Account Could Be Hijacked by an Identity Thief*, TECH@FTC (June 7, 2016), https://www.ftc.gov/news-events/blogs/techftc/2016/06/your-mobile-phone-account-could-be-hijacked-identity-thief; Mary-Ann Russon, *SIM Swap Fraud: The Multi-million Pound Security Issue That UK Banks Won't Talk About*, INT'L BUS. TIMES (Apr. 4, 2016), http://www.ibtimes.co.uk/sim-swap-fraud-multi-million-pound-security-issue-that-uk-banks-wont-talk-about-1553035; Emily Dreyfuss, *@deray's Twitter Hack Reminds Us Even Two-Factor Isn't Enough*, WIRED (June 10, 2016), https://www.wired.com/2016/06/deray-twitter-hack-2-factor-isnt-enough/; Pam Zekman, *2 Investigators: Fraudsters Can Steal Your Phone Number — And More — Through 'Porting'*, CBS CHI. (July 20, 2015), http://chicago.cbslocal.com/2015/07/30/2-investigators-fraudsters-can-steal-your-phone-number-and-more-through-porting/; Jeff Hartman, *Mobile Phone Porting Fraud: The Risk Goes Far Beyond Consumers*, 4DISCOVERY (Mar. 15, 2016), http://www.4discovery.com/2016/03/15/6753/.

rubric of "customer proprietary information." As such, we support the Commission's proposal to allow the permissionless use and disclosure of both CPNI and CPI for fraud (including ATO) prevention and detection.[8] Information about a customer change in account status, such as a user's Mobile Directory Number being moved to another device is often pivotal to detecting ATO. Therefore, the Commission should modify its rules to clarify that carriers may use or disclose *all* types of data covered by Section 222 to combat ATO and other potential harms

To enable the prevention of ATO and other mobile identity fraud, the FCC should also clarify with whom carriers may share data protected by Section 222. Currently, the regulation is silent on this issue, but 47 U.S.C. § 222(d) does not limit the third parties with whom carriers can share protected information.[9] In other words, a carrier may share information covered by Section 222 with *any* third party as reasonably necessary to prevent or respond to fraud.[10] Nonetheless, to prevent confusion, the Commission's regulations should clarify that BIAS providers and traditional CSPs may share or disclose customer CPNI, CPI, pursuant to Section 222(d) with a wide variety of third parties without prior customer consent—provided that the third party uses the protected data only for the purposes of fraud prevention and response. These third parties would include (1) government entities, such as PSAPs or law enforcement; (2) other BIAS providers, CSPs, or network operators; (3) trusted third-party fraud prevention partners; and (4) entities with whom customers have a business relationship, such as financial and health businesses, and who have a need to know in order to protect the consumer. Absent such reassurance from the Commission, BIAS providers and traditional CSPs may continue to be cautious about how and when they can share or disclose data covered by Section 222. In doing so, they will miss opportunities to work with their fraud partners to protect the confidential data and financial assets of their customers and help prevent fraudulent or illegal activity.

---

8 *See BIAS CPNI NPRM* ¶ 117.

9 *See id.* § 222(d).

10 As carriers always do when they release protected information to a third party, a carrier disclosing information pursuant to Section 222(d) would be responsible for taking appropriate steps to ensure that the entities with whom they share information employ reasonable and adequate privacy and data security practices.

Accordingly, we recommend that the Commission revise 47 C.F.R. § 64.2005(d) as follows:

> A telecommunications carrier may use, disclose or permit access to CPNI, *CPI, and customer account status change information without user consent,* to protect the rights or property of the carrier, or to protect users of those services and *the companies they do business with, as well as* other carriers from fraudulent, abusive, or unlawful activity. *Where disclosure of information is permitted by this section, disclosure shall be permitted, unless otherwise prohibited by law, to any third party, including to (i) government entities; (ii) other BIAS and CSP providers and network operators; (iii) third party fraud prevention partners; and (iv) entities that assist in preventing and responding to ATO and other forms of fraud or unlawful activity.*

Respectfully submitted,

Louise L M Tucker